AF IFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
MICHAEL MARCOVICI
SEMYON B. MIZIKOVSKY

Serial No.: 09/592,337

Filed: June 13, 2000

For: AN IMPROVED METHOD FOR AN AUTHENTICATION OF A USER SUBSCRIPTION IDENTITY MODULE

Examiner: J. Kim

Group Art Unit: 2132

Att'y Docket: 2100.001700

Customer No. 046290

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date below:

04.12.05 (Date) Kathy Mans (Signature)

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the Final Office Action dated November 19, 2004. A Notice of Appeal for the above-captioned patent application was filed February 16, 2005, so this Appeal Brief is believed to be timely filed.

A check in the amount of $500.00 is enclosed herein. If the check is inadvertently omitted, The Assistant Commissioner is hereby authorized to deduct the fee for filing this Appeal Brief ($500) from **Williams, Morgan & Amerson's P.C. Deposit Account 50-0786/2100.001700.**

04/15/2005 EFLORES 00000015 09592337
01 FC:1402 500.00 OP

I. REAL PARTY IN INTEREST

The present application is owned by Lucent Technologies, Inc. The assignment of the present application to Lucent Technologies, Inc., is recorded at Reel 11236, Frame 0367.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 7-24 are pending in the application. Claims 7-24 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over admitted prior art in view of Mizikovsky, et al (U.S. Patent No. 5,794,139).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A conventional wireless communication system includes one or more mobile units that may communicate with a serving network. For example, a mobile unit may form a wireless communication link with a base station in the serving network and then transmit and/or receive information over the wireless communication link. The mobile unit may be divided into two portions, a mobile shell and a User Subscription Identity Module (USIM). The mobile shell typically includes the hardware and/or software for establishing communication links and the

USIM typically stores information associated with the subscriber. The USIM may be removed from the mobile shell and used in other mobile shells. When a USIM is inserted into a mobile shell, the information in the USIM is transferred to the mobile shell to allow the mobile unit to gain access to the communication system. See Patent Application, page 3, ll. 1-17.

At times, subscribers to the communication system may transmit and/or receive sensitive and/or private information over the wireless communication link. Consequently, the wireless service provider may implement one or more security schemes, such as an Authentication and Key Agreement (AKA) procedure. When the Authentication and Key Agreement procedure is implemented in a communication system, a mobile unit must be recognized as an authorized user before the mobile unit is given access to the communication system. Accordingly, the USIM generates an integrity key (IK) and a ciphering key (CK) that are used to compute digital signatures and encrypt information transmitted over the communication link. The USIM transfers the integrity key and the ciphering key to the mobile shell, which uses these keys to establish a valid security association with the serving network. See Patent Application, page 4, ll. 4-18. Once the valid security association established and the subscriber is authenticated, encrypted information may be transmitted securely over the communication link.

In some cases, the USIM may be removed from the mobile shell at the conclusion of a secure transmission. For example, a subscriber that has used a USIM card to make a call using a telephone in a taxi may remove the USIM card from the mobile shell at the conclusion of the call. As discussed above, conventional security procedures require the integrity key and the ciphering key to be transferred from the USIM card to the mobile shell. If the telephone is in compliance with current standards, the mobile shell will delete the integrity key and the ciphering key when the USIM card is removed. However, the mobile shell in a rogue telephone

may not delete the ciphering key and/or the integrity key at the conclusion of a call. Thus, fraudulent calls can be made on the rogue phone using the ciphering key and/or the integrity key until the security association is renewed, which may take as long as 24 hours.

To address one or more of the aforementioned problems with the conventional Authentication and Key Agreement procedure, claim 7 sets forth one embodiment of a method of authenticating a user identity module communicatively coupled with a mobile shell having an established security association with a server network. The method set forth in claim 7 includes receiving a first message from the mobile shell, determining a second message based upon the first message and a first key known to the server network and unknown to the mobile shell, and providing the second message to the server network. Claim 16 sets forth another embodiment of a method of authentication by a server network having an established security association with a mobile shell communicatively coupled with a user identity module. The method set forth in claim 16 includes establishing a security association with the mobile shell, receiving a first message from the mobile shell, and authenticating the mobile shell based upon the first message and a first key known to the user identity module and unknown to the mobile shell. Exemplary embodiments of the present invention are shown in Figures 1 and 2 and related discussion on pages 10-14 of the Patent Application.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the single rejection present in this case. The following issue is presented on appeal in this case:

(A) Whether claims 7-24 are obvious over admitted prior art in view of Mizikovsky, et al (U.S. Patent No. 5,794,139).

VII. ARGUMENT

A. Legal Standards

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense

are insufficient to support a finding of obviousness. *Id.* at 1434-35. Moreover, it is the claimed invention, as a whole, that must be considered for purposes of determining obviousness. A mere selection of various bits and pieces of the claimed invention from various sources of prior art does not render a claimed invention obvious, unless there is a suggestion or motivation in the prior art for the claimed invention, when considered as a whole.

It is by now well established that teaching away by the prior art constitutes *prima facie* evidence that the claimed invention is not obvious. *See, inter alia, In re Fine,* 5 U.S.P.Q.2d (BNA) 1596, 1599 (Fed. Cir. 1988); *In re Nielson,* 2 U.S.P.Q.2d (BNA) 1525, 1528 (Fed. Cir. 1987); *In re Hedges,* 228 U.S.P.Q. (BNA) 685, 687 (Fed. Cir. 1986).

B. Claims 7-24 Are Not Obvious over Admitted Prior Art in view of Mizikovsky.

As discussed above, the background section of the specification describes a conventional Authentication and Key Agreement (AKA) procedure. When the conventional AKA procedure is implemented in a mobile unit that includes a mobile shell and a USIM, the USIM generates an integrity key (IK) and a ciphering key (CK), which are used to compute digital signatures and encrypt information transmitted over a communication link. The USIM transfers the integrity key and the ciphering key to the mobile shell, which uses these keys to establish a valid security association with the serving network. See Patent Application, page 4, ll. 4-18. Thus, the integrity key and the cipher key must be known to the mobile shell before the mobile unit can establish a secure connection to the serving network using the conventional AKA procedure. Mizikovsky describes a challenge/response scheme that periodically authenticates a mobile station to a server network.

In the Final Office Action, the Examiner alleges that the admitted prior art teaches a challenge/response scheme that uses a random number generated by a network server and a secret key known by a server network and a user identity module, but unknown to a mobile shell. Appellants respectfully disagree. As discussed above, the integrity key and the cipher key must be known to the mobile shell before the mobile unit can establish a secure connection to the serving network using the conventional AKA procedure. Mizikovsky fails to remedy this fundamental deficiency.

For at least the aforementioned reasons, Appellants respectfully submit that the prior art of record fails to teach all limitations of the invention set forth in independent claims 7 and 16, as well as all claims depending therefrom.

Appellants also submit that the prior art of record fails to provide any suggestion or motivation for modifying the prior art to arrive at the invention set forth in independent claims 7 and 16. To the contrary, the admitted prior art and Mizikovsky both teach away from the invention set forth in independent claims 7 and 16. First, the admitted prior art teaches that the USIM transfers the integrity key and the ciphering key to the mobile shell, which uses these keys to establish a valid security association with the serving network. See Patent Application, page 4, ll. 4-18. Second, Mizikovsky is concerned with automatically generating an authentication key in a mobile station. Mizikovsky also teaches that the mobile station generates a unique challenge response based upon the authentication key that is generated by, and therefore known to, the mobile station. Thus, the admitted prior art and Mizikovsky both teach away from authenticating the mobile shell having an established security association with a server network based upon the first message and a first key known to the user identity module and unknown to the mobile shell.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over the admitted prior art in view of Mizikovsky. Appellants request that the Examiner's rejections of claims 7-24 under 35 U.S.C. 103(a) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 7-24 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 7-24, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: _____

_____

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

1-6. (Canceled)

7. (Previously Presented) A method of authenticating a user identity module communicatively coupled with a mobile shell having an established security association with a server network, the method comprising:

receiving a first message from the mobile shell;

determining a second message based upon the first message and a first key known to the server network and unknown to the mobile shell; and

providing the second message to the server network.

8. (Previously Presented) The method of claim 7, wherein receiving the first message from the mobile shell comprises receiving the first message in response to a challenge interrogation message provided by the server network.

9. (Previously Presented) The method of claim 8, wherein receiving the first message in response to the challenge interrogation message comprises receiving the first message from the mobile shell in response to at least one of a unique challenge interrogation message and a global challenge interrogation message.

10. (Previously Presented) The method of claim 8, wherein receiving the first message comprises receiving a random number provided by the server network.

11. (Previously Presented) The method of claim 10, wherein determining the second message comprises applying a non-reversible algorithmic function to the random number and the first key known to the server network and not known to the mobile shell.

12. (Previously Presented) The method of claim 7, wherein receiving the first message from the mobile shell comprises receiving a first message formed by the mobile shell using a third message and a second key known to the mobile shell and the server network.

13. (Previously Presented) The method of claim 12, wherein receiving the first message from the mobile shell comprises receiving the first message formed by the mobile shell using a third message and an integrity key known to the mobile shell and the server network.

14. (Previously Presented) The method of claim 7, wherein providing the second message to the server network comprises providing the second message to the mobile shell, and wherein the mobile shell is configured to provide at least the second message to the server network.

15. (Previously Presented) The method of claim 7, wherein determining the second message based upon the first key known to the server network and not known to the mobile shell comprises determining the second message based upon an anonymity key known to the server network and not known to the mobile shell.

16. (Previously Presented) A method of authentication by a server network having an established security association with a mobile shell communicatively coupled with a user identity module, the method comprising:

establishing a security association with the mobile shell;

receiving a first message from the mobile shell; and

authenticating the mobile shell based upon the first message and a first key known to the user identity module and unknown to the mobile shell.

17. (Previously Presented) The method of claim 16, wherein receiving the first message from the mobile shell comprises:

providing a second message to the mobile shell after the security association has been established; and

receiving the first message in response to the second message.

18. (Previously Presented) The method of claim 17, wherein providing the second message comprises providing at least one of a unique challenge interrogation message and a global challenge interrogation message.

19. (Previously Presented) The method of claim 17, wherein providing the second message comprises providing a random number.

20. (Previously Presented) The method of claim 19, wherein receiving the first message comprises receiving a first message formed by the user identity module based upon the random number and the first key known to the user identity module and not known to the mobile shell.

21. (Previously Presented) The method of claim 17, wherein authenticating the mobile shell based upon the first message and the first key known to the user identity module and not known to the mobile shell comprises:

determining a fifth message based upon a portion of the second message and the first key known to the user identity module and not known to the mobile shell;

comparing the first message and the fifth message; and

authenticating the mobile shell when a portion of the first message is equal to a portion of the fifth message.

22. (Previously Presented) The method of claim 21, wherein determining the fifth message comprises applying a non-reversible algorithmic function to the portion of the second message and the first key known to the user identity module and not known to the mobile shell.

23. (Previously Presented) at the method of claim 16, wherein receiving the first message comprises receiving a third message formed by the user identity module based upon the first key and a fourth message formed by the mobile shell using a second key known to the mobile shell.

24. (Previously Presented) The method of claim 23, wherein authenticating the mobile shell based upon the first message and the first key known to the user identity module and not known to the mobile shell comprises:

generating a sixth message based upon the first and second keys; and

comparing the first message and the sixth message; and

authenticating the mobile shell when a portion of the first message is equal to a portion of the sixth message.